PRIVACY INTERNATIONAL

Submission to the US Federal Trade Commission on the intersection between privacy, big data, and competition

August 2018

PRIVACY INTERNATIONAL

62 Britton Street
London EC1M 5UY
United Kingdom
Phone +44 (0)20 3422 4321
www.privacyinternational.org

August 20, 2018

Chairman Joseph J. Simons
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Comments in Advance of Federal Trade Commission Hearings on Competition and Consumer Protection in the 21st Century

Dear Chairman Simons,

Privacy International welcomes the opportunity to file these comments in advance of the Federal Trade Commission's public hearings on competition and consumer protection in the 21st century.

Privacy International is a non-profit, non-governmental organisation based in London, the United Kingdom ("UK"), dedicated to defending the right to privacy around the world. Established in 1990, Privacy International undertakes research and investigations into government surveillance and data exploitation in the private sector with a focus on the technologies that enable these practices. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional and international laws that protect privacy around the world. It has litigated or intervened in cases implicating the right to privacy in the courts of the United States, the UK, and Europe. It also strengthens the capacity of partner organisations in developing countries to identify and defend against threats to privacy.

In particular, Privacy International writes to urge the Federal Trade Commission ("FTC") to consider the following issues with respect to topic 4 on the "intersection between privacy, big data and competition."

I. Assessing Data as a Dimension of Competition, and/or as an Impediment to Entry into or Expansion within a Relevant Market

Privacy International encourages the FTC to consider the specific privacy harms that result directly from the dominant positions of certain companies in some digital markets. In particular, we suggest that information and power asymmetry between companies and users have significant implications for the privacy of users and for competition. This

asymmetry is particularly pronounced when companies in dominant positions rely on consent for processing of personal data and/or impose "take it or leave it" terms of services. When faced with a demand to consent to the terms of service and privacy policy by a company in a dominant position, users often have no genuine choice but to accept.[1] The lack of genuine choice is caused by a combination of factors: the significant relevance of network effects in these markets - where the utility of a service increases the more people use it, meaning that entrants require a 'critical mass' of users in order to compete, while users may only use the competing service when it has been generally adopted; lock-in of users; lack of alternatives and of interoperability[2]; imposition of terms and conditions that lock users into using services with poor privacy safeguards.[3]

As summarised by the European Data Protection Supervisor, the EU independent data protection authority, "dominant companies in the digital market are able to foreclose new entrants from competing on factors which could benefit the rights and interests of individuals, and may impose unfair terms and conditions which abusively exploit consumers. An apparent growing imbalance between web-based service providers and consumers may diminish choice, innovation and the quality of safeguards for privacy. This imbalance may also raise the effective price - in terms of personal data disclosure - far beyond what might be expected in fully competitive markets."[4]

Privacy International also believes that privacy harms are directly caused by the business models of companies in dominant positions, which increasingly rely on the availability of users' data. In a recent draft white paper on "Potential Policy Proposals for Regulation of Social Media and Technology Firms," Senator Mark Warner noted that "user data is increasingly the single most important economic input in information markets".[5] With the increasing development and integration of artificial intelligence technologies, it is likely that users' data will become even more important for these companies.

---

[1] As noted by the European Data Protection Board (formerly the Article 29 Working Party): "Imbalances of power are not limited to public authorities and employers, they may also occur in other situations. . . . [C]onsent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will." Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, Nov. 28, 2017, available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

[2] In this context, see Standard Glossary of Software Engineering Terminology" (IEEE 610) of the Institute of Electrical and Electronics Engineers: Interoperability is[t]he ability of two or more systems or components to exchange information and to use the information that has been exchanged ...".

[3] For example, last year the Italian Competition Authority fined WhatsApp for forcing its users to accept new terms and conditions that led to the sharing of personal data with Facebook. That decision is available in Italian here: http://www.agcm.it/component/joomdoc/allegati-news/PS10601_scorrsanz_omi.pdf/download.html.

[4] European Data Protection Supervisor Opinion on coherent enforcement of fundamental rights in the age of big data, Opinion 8/2016, Sept. 23, 2016, available at https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf.

[5] U.S. Senator Mark R. Warner, draft White Paper, Potential Policy Proposals for Regulation of Social Media and Technology Firms, available at https://assets.documentcloud.org/documents/4623358/PlatformPolicyPaper.pdf.

The European Data Protection Supervisor has suggested that "the harvesting of personal data is, in the digital sphere, a proxy for price."[6] However, when assessing market power, competition authorities have tended to focus on price and outputs, giving little to no consideration to other factors affecting competition, such as quality, innovation and the implications for the exercise of certain fundamental rights, such as the right to privacy. This narrow approach misses the increasingly important competition implications of the collection of personal data, particularly when done at scale. It also fails to take into consideration the multiple effects that gaining personal data has on certain types of digital services. For example, the network effects of the online market can raise the importance of gaining or losing a user because of the importance of personal data (at scale) for the functioning of certain algorithms, such as those that underpin the effectiveness of targeted advertising.[7]

In analysing this issue, Privacy International encourages the FTC to consider how to assess the value of personal data in digital markets, beyond pure monetary terms, and in particular the data-driven network effects of the collection of personal data.

II. Assessing Competition based on Privacy and Data Security Attributes and the Importance of this Competition to Consumers and Users

Privacy International welcomes the FTC's intention to assess the impact that competition has on privacy. As recent research has demonstrated, users demand both confidentiality and security of their digital communications and protection of their personal data.[8] In a competitive market, it should be expected that the level of data protection offered to individuals would be subject to genuine competition, i.e. companies would compete to offer privacy friendly services.[9]

However, in a data-intensive digital market characterised by increased corporate concentration, companies in a dominant position have no incentive to adopt businesses models and practices that enhance individuals' privacy, and they may seek to exclude any

[6] European Data Protection Supervisor Opinion on coherent enforcement of fundamental rights in the age of big data, *supra*.

[7] Academics have described ten implications of data-driven network effects, which are relevant to this analysis. See Maurice Stucke and Allen Grunes, Big data and competition policy, Oxford University Press, 2016, pages 200-205.

[8] For evidence of concerns on the current lack of strong privacy and data protection laws, see in the United States, National Telecommunications and Information Administration, "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities, May 13, 2016, https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may- deter-economic-and-other-online-activities, and in the European Union, European Commission, Eurobarometer on ePrivacy, Dec. 19, 2016, available at https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy.

[9] In its 2014 assessment of the proposed merger of Facebook and WhatsApp (Case No. COMP/M.7217), the European Commission acknowledged that "competition on privacy" exists. It stated that "apps compete for customers by attempting to offer the best communication experience," including with respect to "privacy and security, the importance of which varies from user to user but which are becoming increasingly valued, as shown by the introduction of consumer communications apps specifically addressing privacy and security issues." For additional authorities on this point, see Francisco Costa-Cabral & Orla Lynskey, Family ties: the intersection between data protection and competition in EU law, Common Market Law Review, 54: 11-50, 2017, available at http://eprints.lse.ac.uk/68470/7/Lynskey_Family%20ties%20the%20intersection%20between_Author_2016_LSERO.pdf.

privacy enhancing players from any of the markets where they can exert market power. For example, Google's ban of mobile ad-blocker Disconnect (among other services) from the Google Play Store recently led to a case before the European anti-trust authority and a record $5.1 billion fine against the company.[10] As two leading academics in the UK state on this point, companies "may already be exercising their market power to foment consumers' supposed lack of interest for data protection: competition on this parameter may be suppressed, as a result of which the current data protection conditions offered do not reflect the competitive level. An analogy could be made to situations where an undertaking has already exercised its power to impose high prices, and thus the current price does not reflect a competitive price… [I]t may be market power that is preventing such competition from emerging."[11]

Privacy International believes that privacy standards, including the protection of personal data and data security, should be part of any assessment of the quality of a digital service for the purpose of determining competitiveness of a market. We encourage the FTC to develop explicit guidance on this point.

III. The Benefits and Costs of Privacy Regulation, including the Effect of such Regulation on Innovation, Product offerings, and Other Dimensions of Competition and Consumer Protection

Companies exploiting personal data often view privacy and data protection legislation as a threat to their business models. Their responses to the European Union's General Data Protection Regulation demonstrates this stance. In its 2016 Annual report, Facebook noted how its business may be negatively affected by privacy, data protection, consumer and competition laws.[12] Alphabet Inc.'s 2017 Annual Report to the US Securities and Exchange Commission notes similar concerns and specifically states in relation to data protection regulation that "these legislative and regulatory proposals, if adopted . . . could, in addition to the possibility of fines, result in an order requiring that we change our data practices, which could have an adverse effect on our business and results of operations. Complying with these various laws could cause us to incur substantial costs or require us to change our business practices in a manner adverse to our business."[13]

---

[10] See Adam Satariano & Jack Nicas, E.U. Fines Google $5.1 Billion in Android Antitrust Case, N.Y. Times, July 18, 2018, https://www.nytimes.com/2018/07/18/technology/google-eu-android-fine.html ; Ingrid Lunden, Disconnect.Me Files Antitrust Case Against Google in Europe Over Banned Anti-Malware Android App, TechCrunch, June 2, 2015, https://techcrunch.com/2015/06/02/disconnect-me-files-antitrust-case-against-google-in-europe-over-banned-anti-malware-android-app/.

[11] Costa-Cabral & Lynskey, Family ties: the intersection between data protection and competition in EU law, *supra*.

[12] Facebook, Annual Report 2016, available at http://www.annualreports.com/HostedData/AnnualReportArchive/f/NASDAQ_FB_2016.pdf ("Our business is subject to complex and evolving U.S. and foreign laws and regulations regarding privacy, data protection, competition, consumer protection, and other matters. Many of these laws and regulations are subject to change and uncertain interpretation, and could result in claims, changes to our business practices, monetary penalties, increased cost of operations, or declines in user growth or engagement, or otherwise harm our business."

[13] See Alphabet Inc., Form 10-K, available at https://abc.xyz/investor/pdf/20171231_alphabet_10K.pdf.

Dominant market players often criticise data protection legislation on the grounds that it would harm smaller companies with smaller compliance teams. A more accurate description, however, would be that it threatens their own, current business model. Privacy International therefore believes that privacy and data protection standards should be used to help assess the competitiveness of a market (see above).

Further, Privacy International notes that privacy and data protection legislation serve the purpose of limiting certain negative market behaviour even if such behaviour is technically compliant with competition law. Privacy is a fundamental human right, recognised by numerous international human rights instruments, including in Article 17 of the International Covenant of Civil and Political Rights, which has been ratified by the US. Data-protection laws are also an increasingly important aspect of international law, including with respect to securing the right to individual privacy under international human rights law.[14] Accordingly, personal data "cannot be conceived as a mere economic asset"[15] and therefore privacy and data protection laws must be construed as capable of limiting the application of competition law, when such application would result in a violation of users' rights to privacy and data protection.

There is increased recognition of the need to consider data protection standards by competition authorities. For example, the German competition authority has noted that "where access to personal data of users is essential for the market position of a company [here, Facebook], the question of how that company handles the personal data of its users is no longer only relevant for data protection authorities. It becomes a relevant question for the competition authorities, too."[16]

Privacy International encourages the FTC to analyse the implications of the interplay between privacy and competition laws, for example by developing guidance on how privacy and data protection standards can be used to help determine the "harm" relevant for assessing mergers and abuses of dominance.

IV. Competition and Consumer Protection Implications of Use and Location Tracking Mechanisms

Privacy International welcomes the interest of the FTC in the competition and consumer protection implications of use and location tracking mechanisms.

Most websites include embedded code, which collects data that can reveal the identity and interests of those visiting those sites. However, consumer tracking is no longer limited to

[14] For more details, see Brief of Privacy International, Human and Digital Rights Organizations, and International Legal Scholars as *Amici Curiae* in support of Respondent, United States v. Microsoft Corp., No. 17-2, 18 Jan. 2018, available at https://www.privacyinternational.org/sites/default/files/2018-03/U.S.%20v.%20Microsoft%20Brief%20FINAL.pdf.

[15] European Data Protection Supervisor Opinion on coherent enforcement of fundamental rights in the age of big data, Opinion 8/2016, *supra*.

[16] Quoted in Slaughter and May, Facebook / Germany – a new frontier for privacy and competition?, March 2018, https://www.slaughterandmay.com/media/2536711/facebook-germany-a-new-frontier-for-privacy-and-competition.pdf.

cookies, but has advanced to more sophisticated techniques, such as cross-device tracking and device fingerprinting, which are much harder to identify and to escape.[17] At the same time, websites, mobile applications, and smart devices routinely share data with countless of unnamed "third parties" for purposes of advertisement.[18]

Each of these individual data points may not seem particularly revealing on their own, but a review of published academic papers conducted by Privacy International found numerous examples demonstrating how seemingly disparate data points can be combined to create a meaningful profile of a person. These examples further show how easily individuals can be identified, re-identified, tracked and profiled.[19]

Some specific examples of data points from a mobile phone, which can be combined to track and profile a person include:

- Using only four data points containing a timestamp and location from cell phone data, researchers were able to successfully track 95% of people;
- Researchers were able to use knowledge of installed smartphone apps to figure out users' personal information, including gender, "religion, relationship status, spoken languages, countries of interest, and whether or not the user is a parent of small children;"
- Using cell phone usage data (e.g. call logs, bluetooth, cell towers, app usage, and phone status), researchers were able to make highly accurate predictions of users' friendships;
- Researchers used cell phone call data to highly accurately classify contacts as social, family, or work-related;
- In a study that tracked the cell phone usage (e.g. call logs, bluetooth, and SMS) of 26 couples, researchers were able to predict the spending behavior of those couples.

Privacy International encourages the FTC to consider the privacy implications of practices such as profiling as well as automated decision making based on such profiling.[20] These practices, which are increasing across different sectors of commerce, challenge existing privacy and data protection standards in the US and elsewhere. The widespread availability of data, the increased ability to link data, and advances in data processing

[17] See Tactical Tech's tool, Trackography, https://myshadow.org/trackography

[18] See Katarzyna Szymielewicz & Bill Budington, The GDPR and Browser Fingerprinting: How It Changes the Game for the Sneakiest Web Trackers, EFF, June 19, 2018, https://www.eff.org/deeplinks/2018/06/gdpr-and-browser-fingerprinting-how-it-changes-game-sneakiest-web-trackers); Reuben Binns et al., Measuring third party tracker power across web and mobile, Feb. 7, 2018, available at https://arxiv.org/abs/1802.02507.

[19] Privacy International, Examples of Data Points Used in Profiling, https://privacyinternational.org/sites/default/files/2018-04/data%20points%20used%20in%20tracking_0.pdf.

[20] Profiling is about recognizing patterns, revealing correlations and making inferences. Through profiling, highly sensitive information can be inferred, derived or predicted from other non-sensitive data. As a result, data about an individual's behaviour can be used to generate previously unknown information about someone's likely identity, attributes, behaviour, interests, or personality. This includes information revealing or predicting an individual's likely racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual behaviour or sexual orientation.

technology are all contributing to the increasing use of profiling by private and public bodies across a range of sectors, including banking and finance, healthcare, taxation, insurance, marketing and advertising, and criminal justice and policing.

Because of the inherently probabilistic nature of profiling, individuals are frequently misidentified, misclassified or misjudged as having certain attributes or characteristics. Some individuals belong to groups of society that are systematically misidentified, misclassified, or misjudged.[21]

From a competition perspective, profiling may also lead to price[22] and other forms of discrimination based on a user's profile. An individual or a segment of the population can be excluded from receiving information or opportunities, or be targeted with "negative" advertising, which might reinforce existing social disadvantages. For example, a lawsuit is currently pending against Facebook for reportedly allowing advertisers to discriminate against legally protected groups.[23]

As noted by the European Data Protection Board (a body composed of composed of representatives of the EU national data protection authorities, formerly the Article 29 Working Party), "advances in technology and the capabilities of big data analytics, artificial intelligence and machine learning have made it easier to create profiles and make automated decisions with the potential to significantly impact individuals' rights and freedoms."[24] This conclusion echoes the UN Human Rights Council's 2017 resolution, which states that "automatic processing of personal data for individual profiling may lead to discrimination or decisions that have the potential to affect the enjoyment of human rights, including economic, social and cultural rights."[25]

V. Lack of Transparency of the Data Ecosystem

Privacy International encourages the FTC to address the lack of transparency and related lack of consumer control over what happens to personal data in the digital market. The lack of transparency exists at three levels: users' level, process level and market level. Opacity at each level has implications for competition, consumer protection and privacy.

---

[21] For some examples, see Privacy International, Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR, https://privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf

[22] See Aniko Hannak et al., Measuring Price Discrimination and Steering on E-commerce Web Sites, in Proceedings of the 2014 Conference on Internet Measurement Conference, 2014, pp. 305-318; Jakub Mikians et al., Detecting Price and Search Discrimination on the Internet, in Proceedings of the 11th ACM Workshop on Hot Topics in Networks, 2013, pp. 79-84.

[23] See Julia Angwin and Ariana Tobin, Fair Housing Groups Sue Facebook for Allowing Discrimination in Housing Ads, ProPublica, Mar. 27, 2018, https://www.propublica.org/article/facebook-fair-housing-lawsuit-ad-discrimination. The complaint is available here: https://www.documentcloud.org/documents/4424703-NFHA-v-Facebook-Complaint-W-Exhibits.html.

[24] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Oct. 3, 2017, available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

[25] UN Human Rights Council, Resolution, The right to privacy in the digital age, UN doc. A/HRC/RES/34/7, Mar. 22, 2017.

At the users' level, consumers do not know how their personal data is collected, used and shared with other parties; nor do they know when they have been tracked and profiled. Three common misconceptions characterise the ways in which many consumers understand data. Even when consumers "consent" to cookies or other forms of tracking on websites for marketing purposes, the insights that can be gleaned from such data, and the purposes for which these insights are being used, often exceed users' knowledge or consent.

First of all, consumers often assume that the company is using data that they have more or less consciously shared. But increasingly, companies are collecting and using data about users that they are not aware is being collected and used. When all of these various data points are combined, they can reveal a shockingly granular and intimate image of a person's life.[26] Second, consumers often mistakenly assume that data that is not associated with their name is truly anonymous. For example, journalists from the German public broadcaster NDR were able to identify the sexual preference and medical history of judges and politicians from "anonymised" browsing histories. Finally, consumers are often led to believe that their data is only being collected for marketing purposes. However, the complex ecosystem of companies and brokers that drive the ad-supported internet is increasingly being tapped into by all sorts of actors. For example, in the UK, the popular UK parenting blog 'Emma's diary' collected data for marketing purposes and then shared this data with the data broker arm of Experian, which in turn sold it to a political party in the UK.[27]

At the process level, profiling itself can be highly opaque, in particular if it is based on advanced processing, such as machine learning. Depending on the kinds of algorithms used, whether these are learning, and how they are trained, it can be difficult, even for the designers of such systems, to understand how or why an individual has been profiled in any particular way, whether that profile is accurate, or why a system has made a particular decision.

And finally, at the market level, it is increasingly difficult to track the way data is shared by companies, although there are increasing efforts to document the complexity and opacity of the data ecosystem[28] and some legislative initiatives have emerged seeking to provide more transparency and control over data brokers.[29]

---

[26] See Privacy International, How do data companies get our data, May 25, 2018, https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data

[27] See Information Commissioner's Office, Emma's Diary fined £140,000 for selling personal information for political campaigning, Aug. 9, 2018, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/08/emma-s-diary-fined-140-000-for-selling-personal-information-for-political-campaigning/.

[28] See Wolfie Christl, Corporate Surveillance in Everyday Life - How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions, Cracked Labs, June 2017, http://crackedlabs.org/en/corporate-surveillance.

[29] See, for example, Vermont's Data Broker Regulatory Regime, enacted on May 22, 2018, https://legislature.vermont.gov/assets/Documents/2018/Docs/BILLS/H-0764/H-0764%20As%20Passed%20by%20Both%20House%20and%20Senate%20Unofficial.pdf.

Privacy International believes that such lack of transparency has significant negative implications in relation to competition, and the protection of users' privacy. In fact, there is arguably an incentive for some companies to adopt business models that are less transparent and less auditable by antitrust authorities so as to disempower both competitors and consumers.

Privacy International encourages the FTC to consider how this lack of transparency negatively affects the capacity of regulators, including anti-trust authorities, to assess competitive and consumer harms.

- - -

The above considerations reflect some of the key Privacy International's ongoing concerns on the exploitation of personal data by companies. By looking at the privacy, data protection, consumer protection and competition laws, the FTC has a significant opportunity to interpret these laws in ways that provide effective protection to users. Privacy International is prepared to provide additional information on these issues throughout the term of the hearings.

Yours sincerely,

Tomaso Falchetta
Advocacy and Policy Team Lead
Privacy International